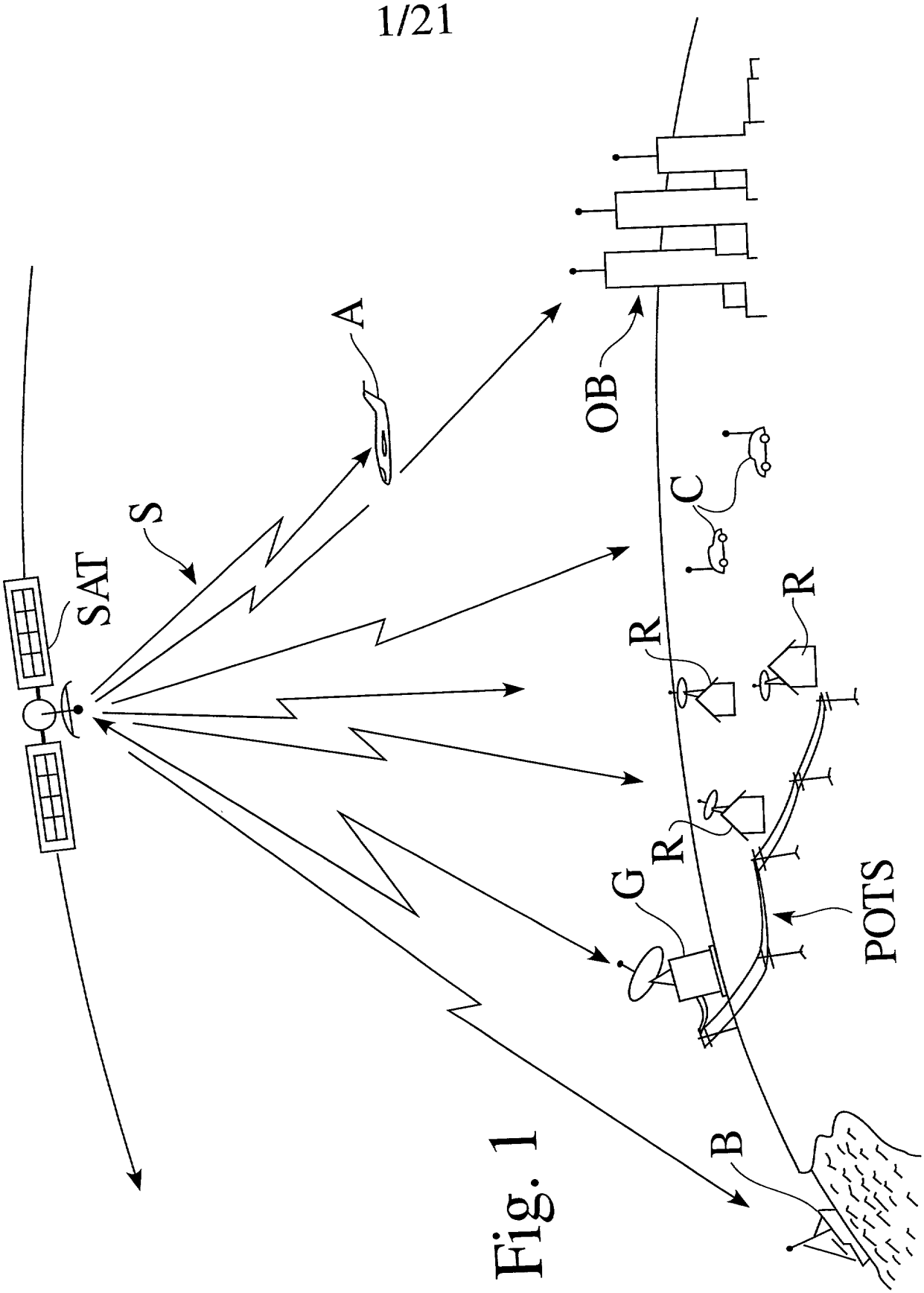


Fig. 1

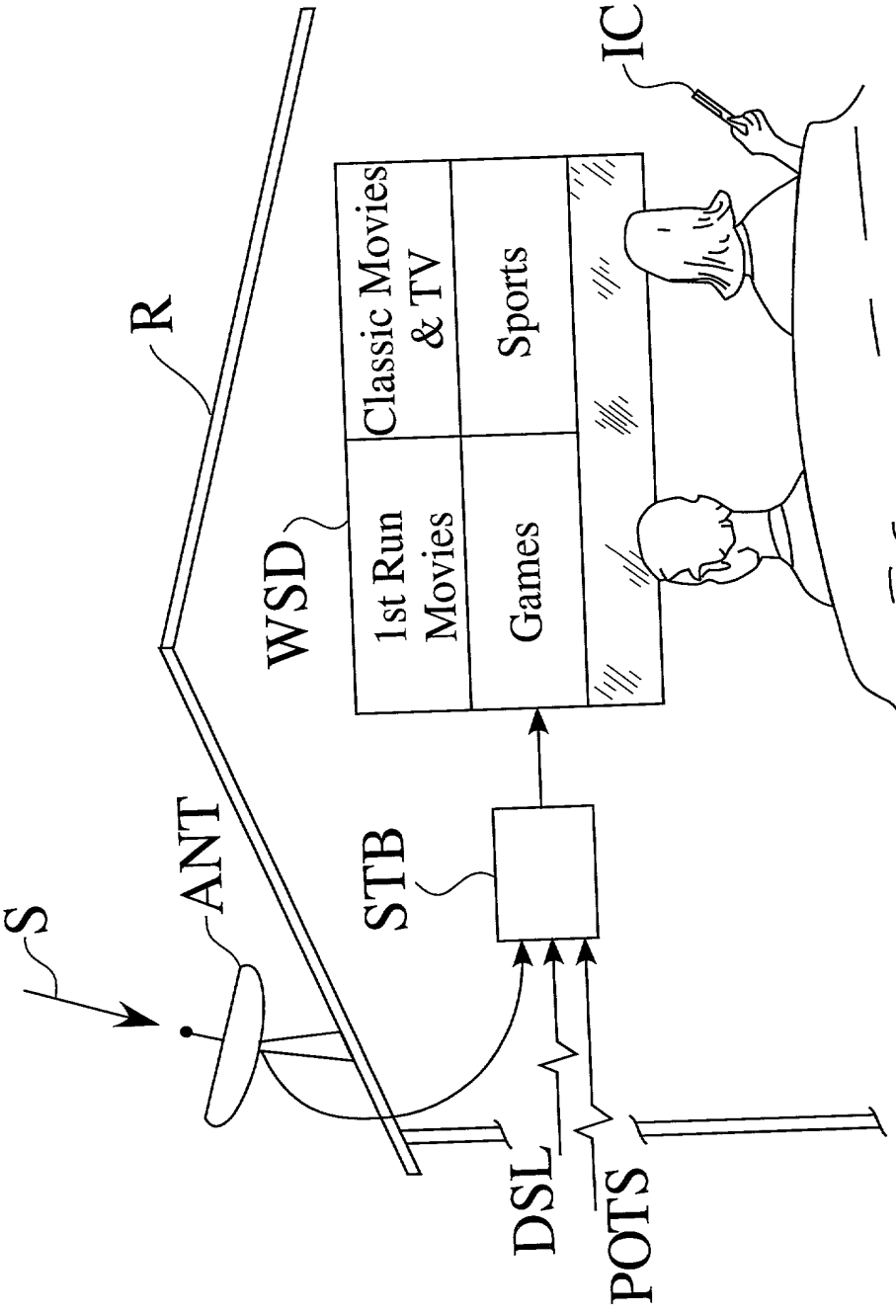

S
ANT
R
STB
WSD
1st Run Movies
Games
Classic Movies & TV
Sports
IC
DSL
POTS

Fig. 2

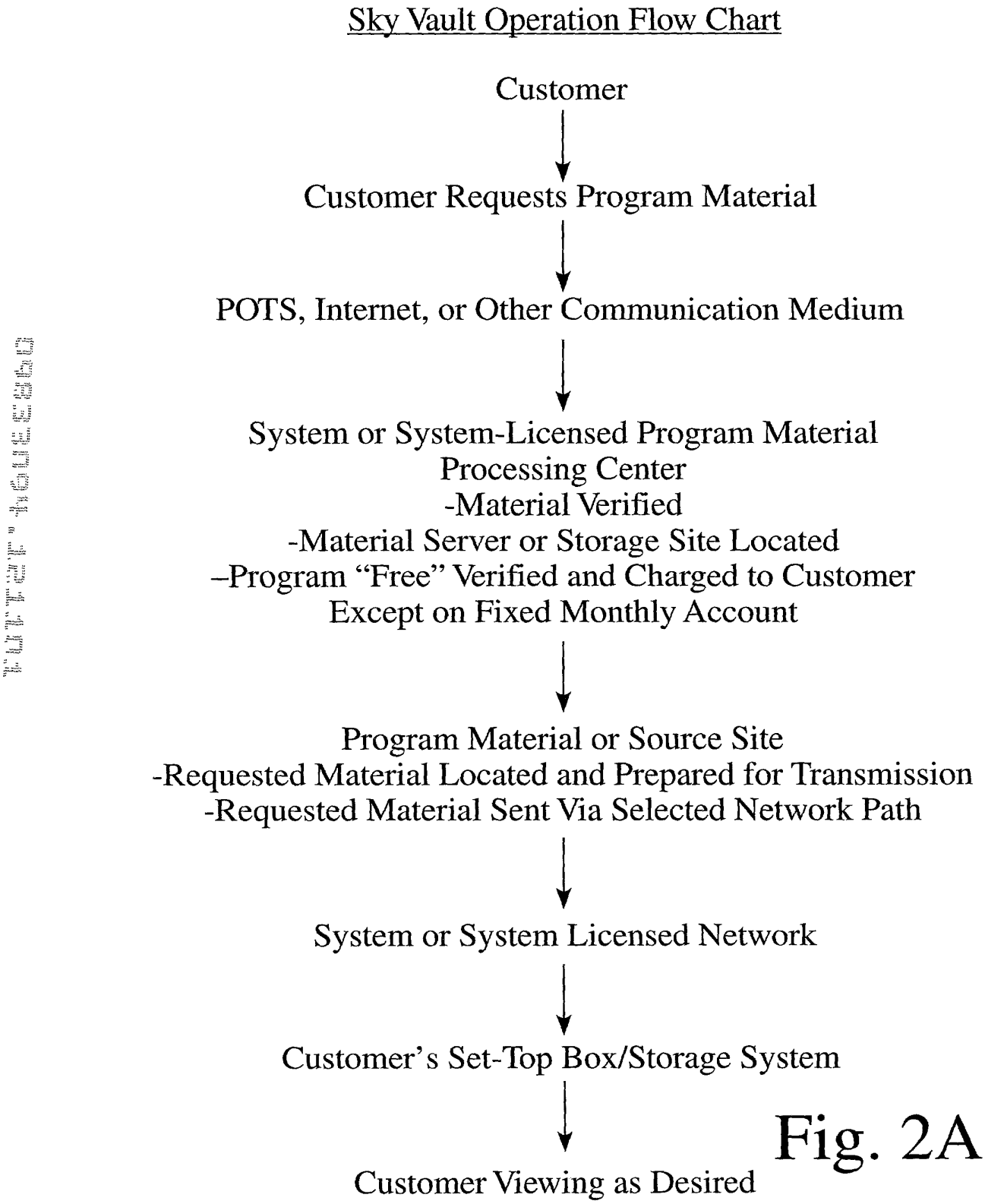

Sky Vault Operation Flow Chart
Customer
Customer Requests Program Material
POTS, Internet, or Other Communication Medium
System or System-Licensed Program Material Processing Center
-Material Verified
-Material Server or Storage Site Located
–Program "Free" Verified and Charged to Customer Except on Fixed Monthly Account
Program Material or Source Site
-Requested Material Located and Prepared for Transmission
-Requested Material Sent Via Selected Network Path
System or System Licensed Network
Customer's Set-Top Box/Storage System
Customer Viewing as Desired

Fig. 2A

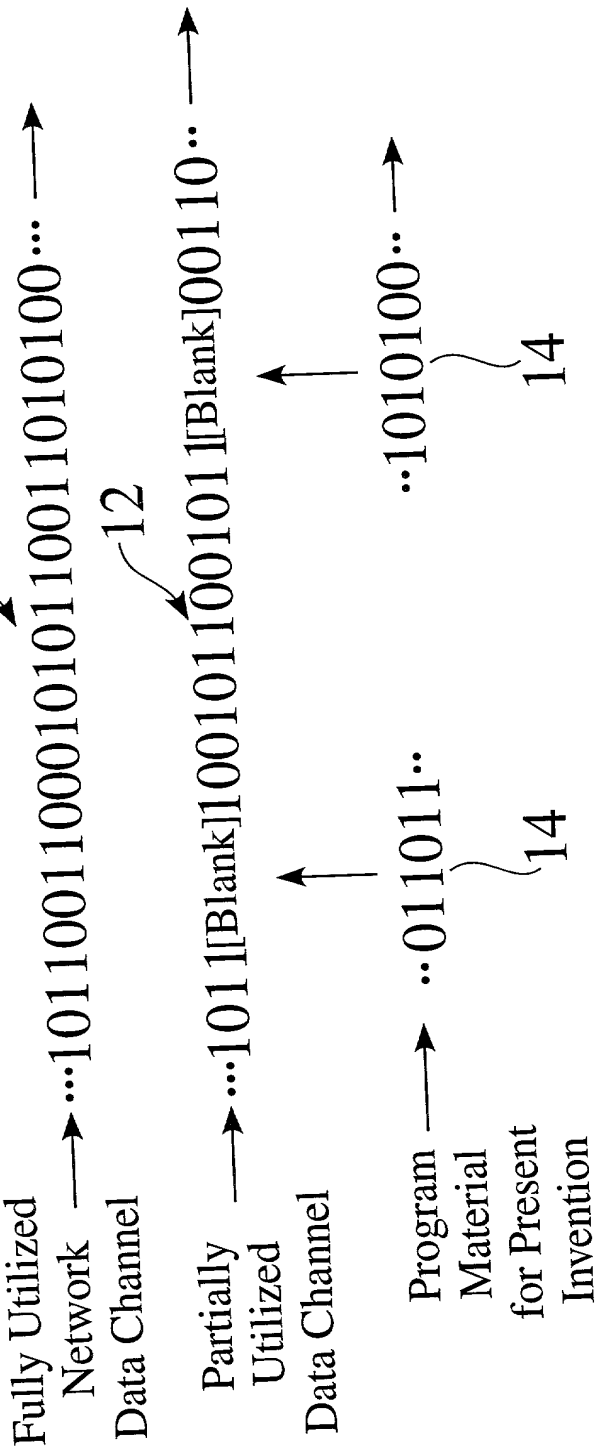

10
12
Fully Utilized Network Data Channel
Partially Utilized Data Channel
Program Material for Present Invention
··1011001100010101100110101100··
··1011[Blank]1001011001011[Blank]001110··
··0110111··
··1010100··
14
14

Fig. 3

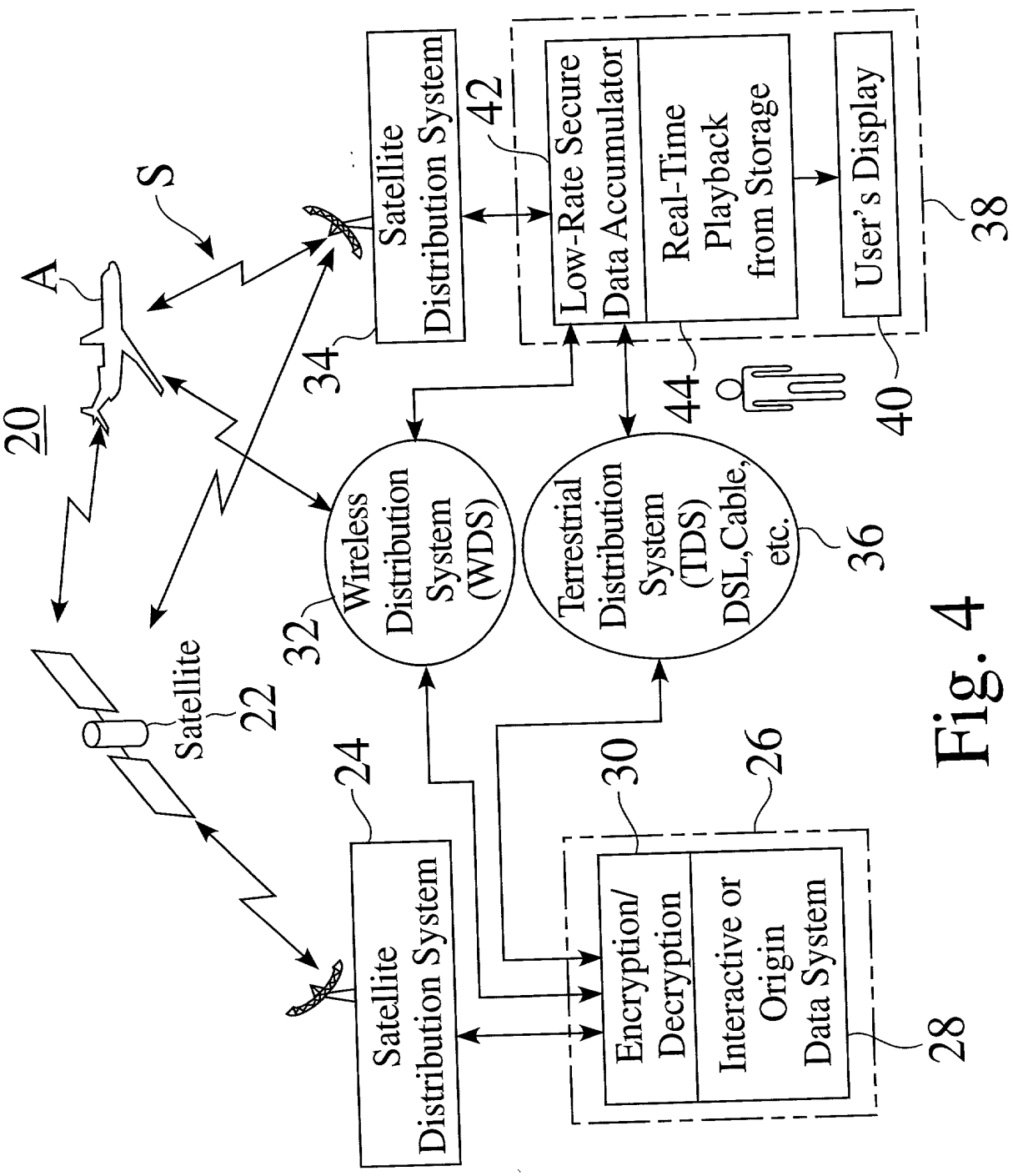

20
A
S
Satellite
22
24
Satellite Distribution System
Wireless Distribution System (WDS)
32
Terrestrial Distribution System (TDS) DSL,Cable, etc.
36
30
26
Encryption/ Decryption
Interactive or Origin Data System
28
34
Satellite Distribution System
42
Low-Rate Secure Data Accumulator
Real-Time Playback from Storage
44
User's Display
40
38

Fig. 4

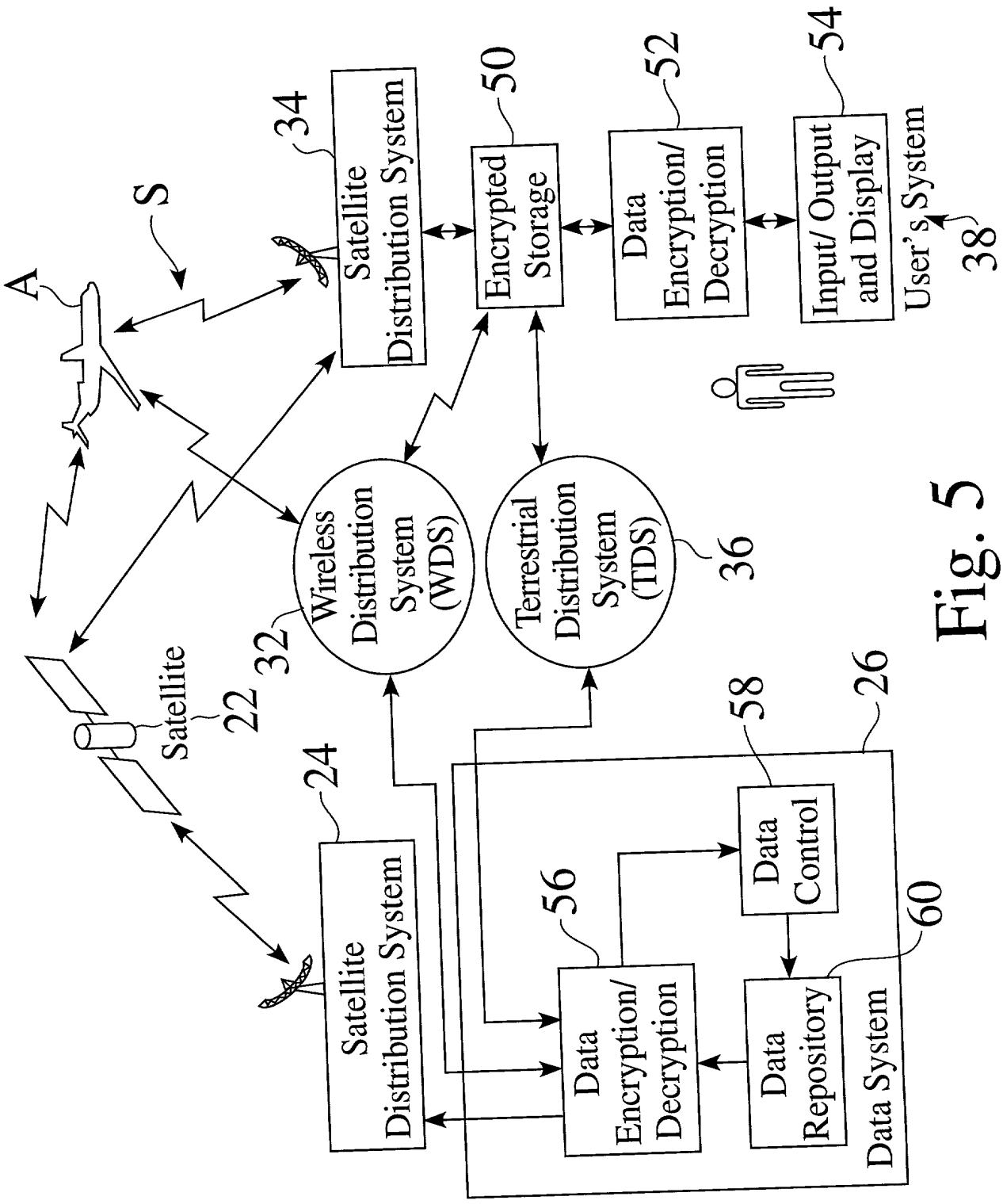

A
S
Satellite
22
24
Satellite Distribution System
Satellite Distribution System
34
Wireless Distribution System (WDS)
32
Terrestrial Distribution System (TDS)
36
Encrypted Storage
50
Data Encryption/ Decryption
52
Input/ Output and Display
54
User's System
38
Data System
26
Data Encryption/ Decryption
56
Data Control
58
Data Repository
60

Fig. 5

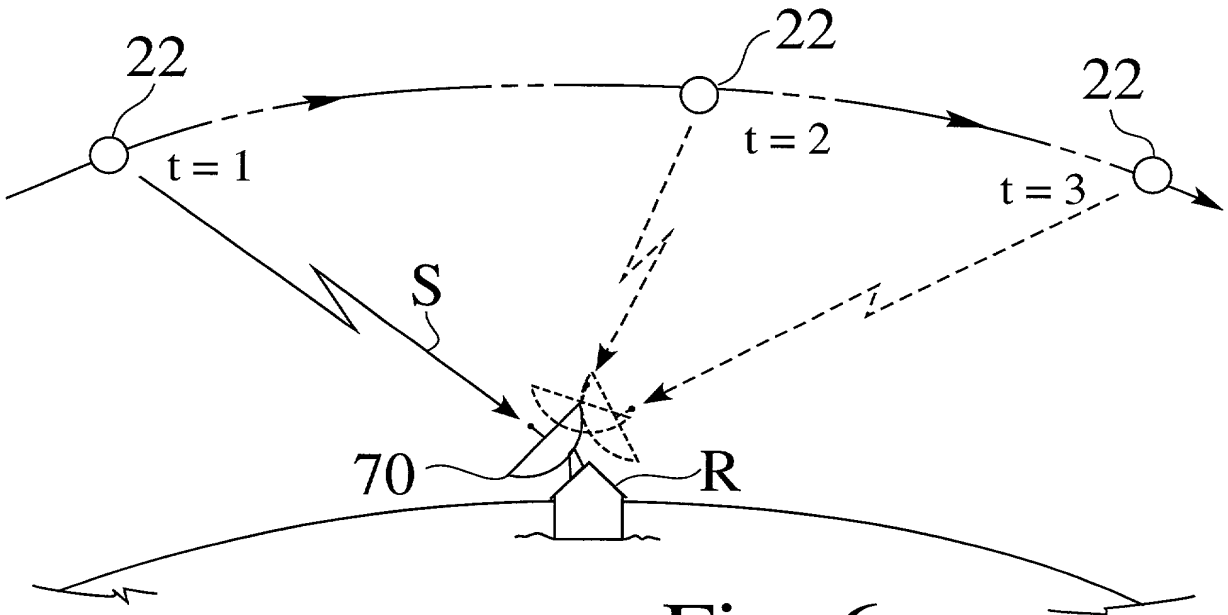


Fig. 6

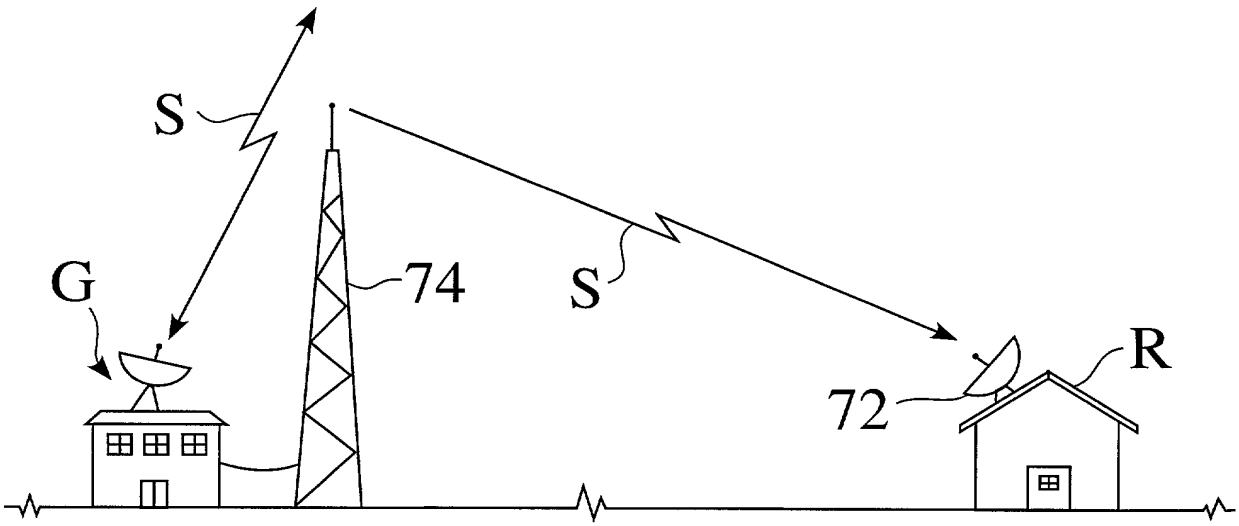


Fig. 7

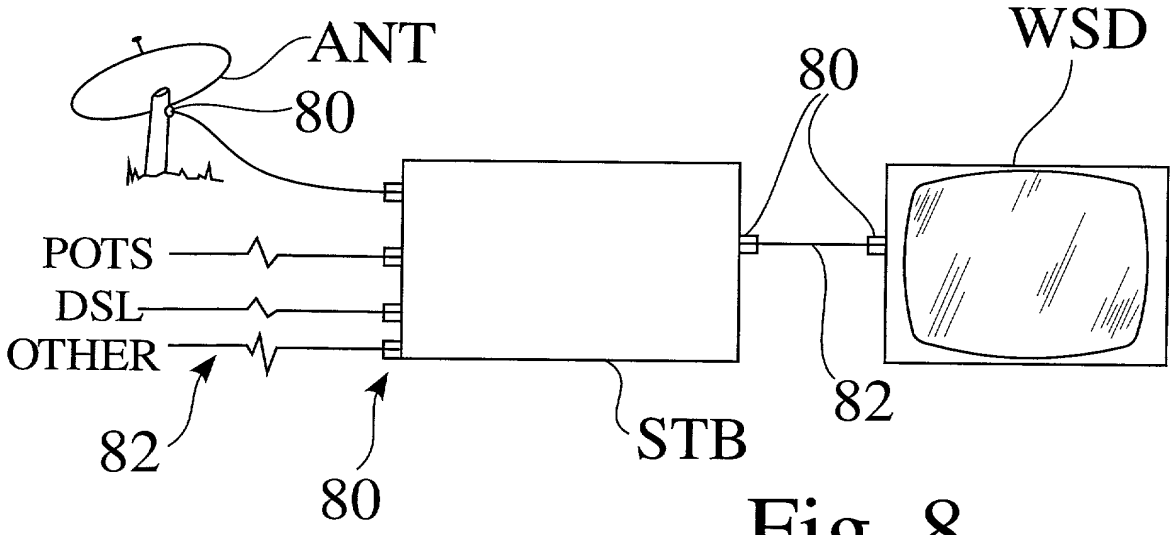

ANT
80
WSD
80
POTS
DSL
OTHER
82
80
STB
82

Fig. 8

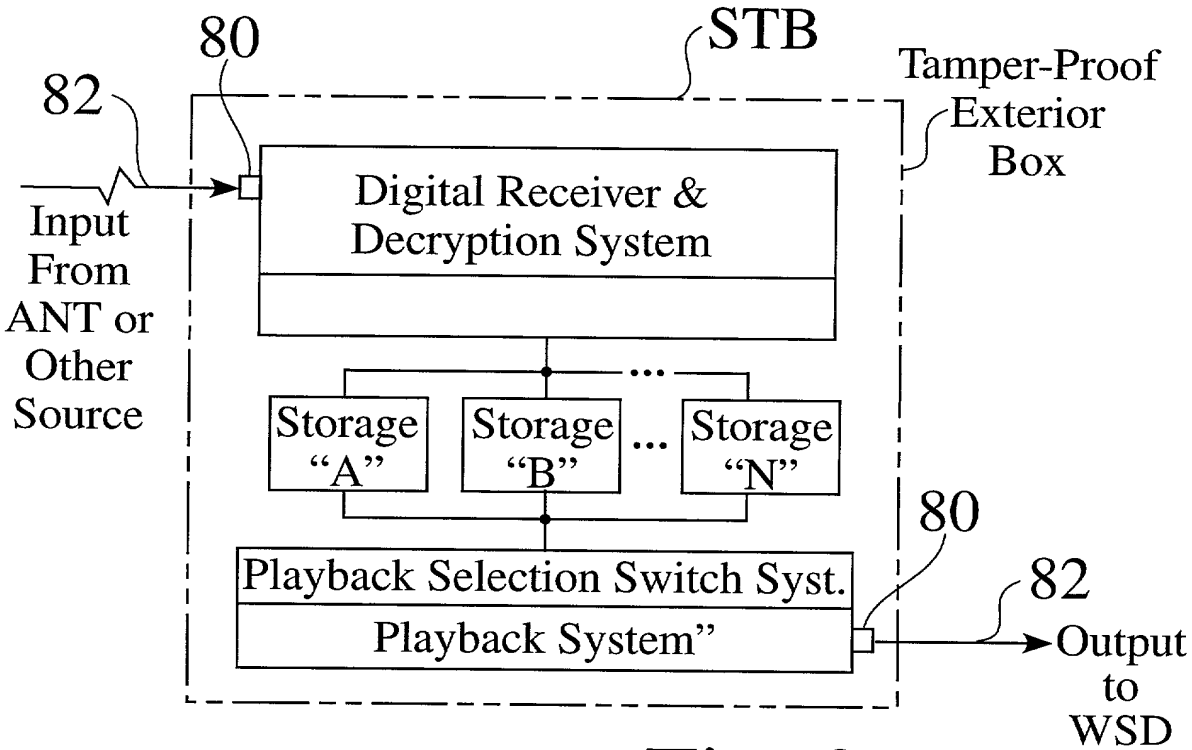

80
STB
82
Tamper-Proof
Exterior
Box
Input
From
ANT or
Other
Source
Digital Receiver &
Decryption System
Storage
"A"
Storage
"B"
Storage
"N"
80
Playback Selection Switch Syst.
Playback System"
82
Output
to
WSD

Fig. 9

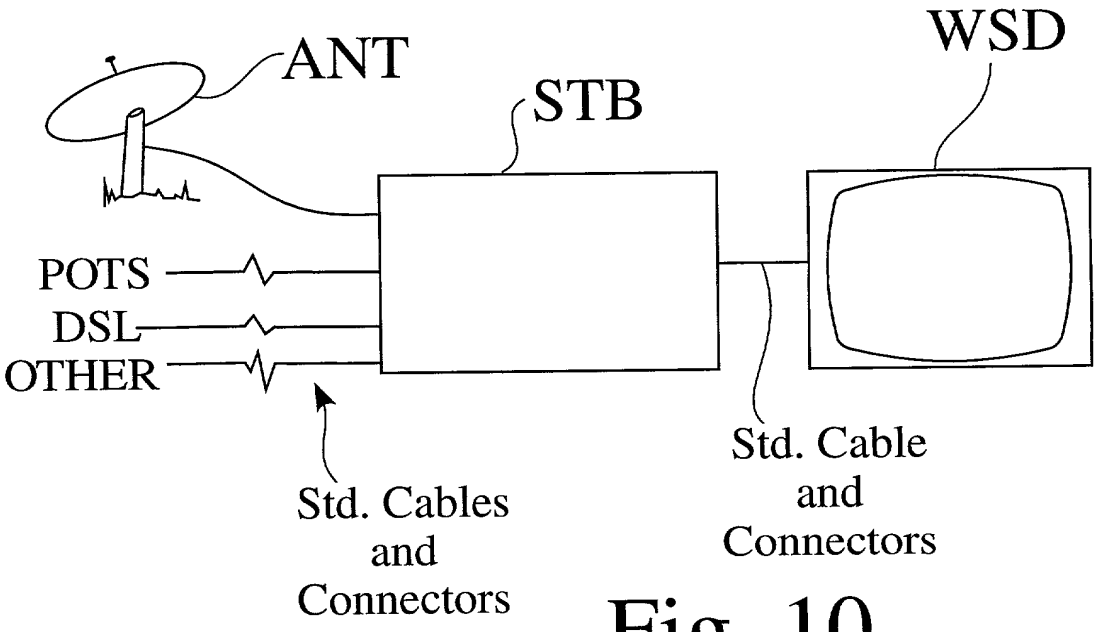

ANT
STB
WSD
POTS
DSL
OTHER
Std. Cables and Connectors
Std. Cable and Connectors

Fig. 10

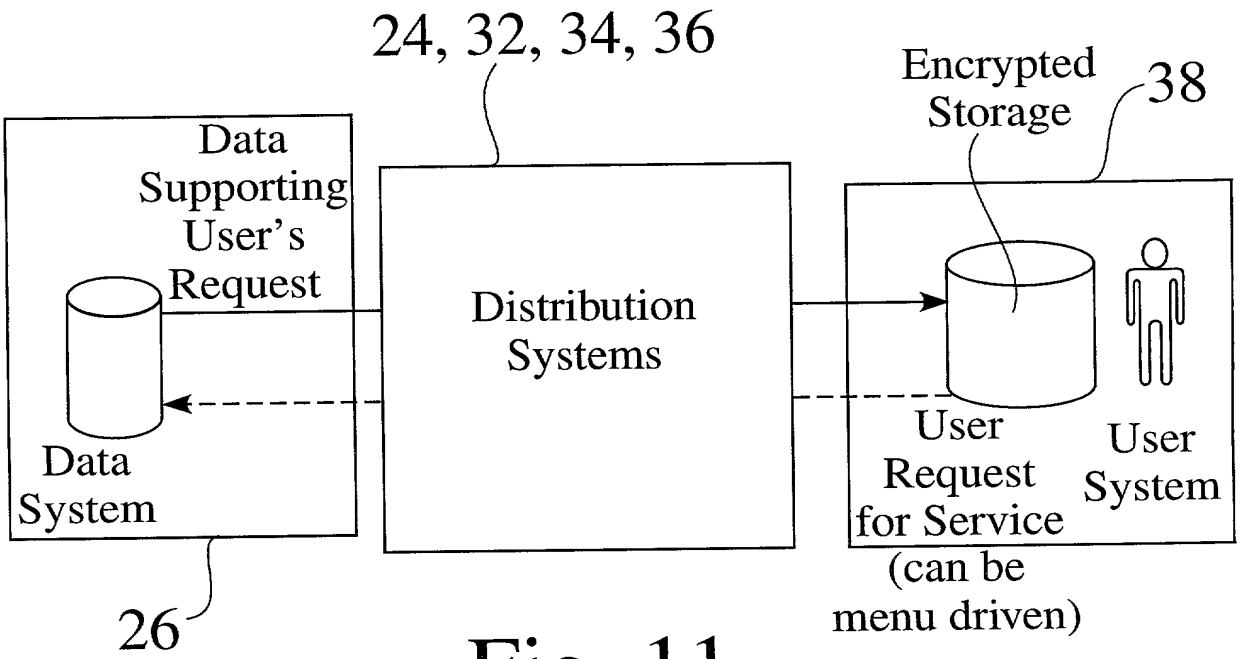

24, 32, 34, 36
Encrypted Storage
38
Data Supporting User's Request
Distribution Systems
Data System
User Request for Service
User System
(can be menu driven)
26

Fig. 11

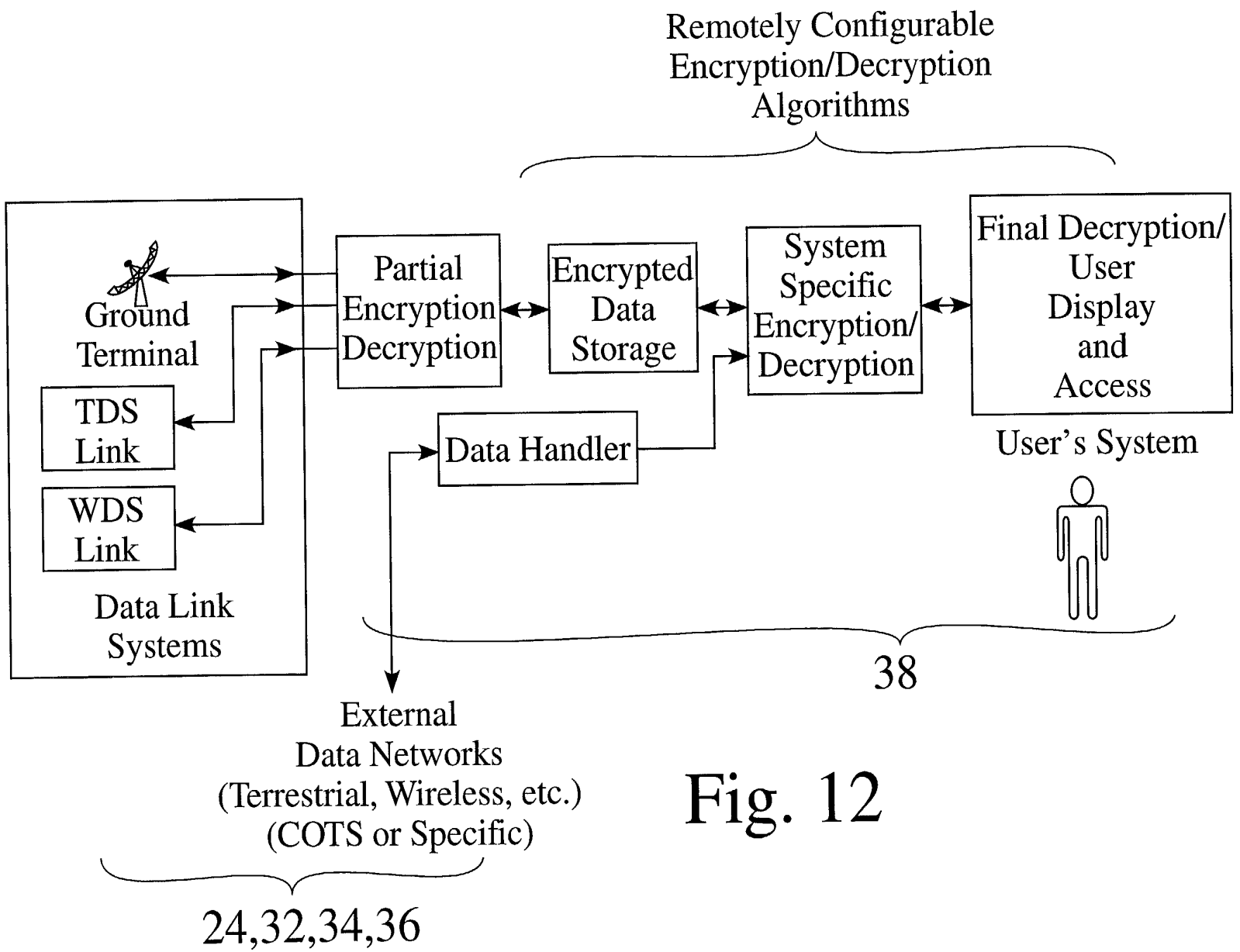

Remotely Configurable
Encryption/Decryption
Algorithms
Ground
Terminal
TDS
Link
WDS
Link
Data Link
Systems
Partial
Encryption
Decryption
Encrypted
Data
Storage
System
Specific
Encryption/
Decryption
Final Decryption/
User
Display
and
Access
User's System
Data Handler
38
External
Data Networks
(Terrestrial, Wireless, etc.)
(COTS or Specific)
24,32,34,36

Fig. 12

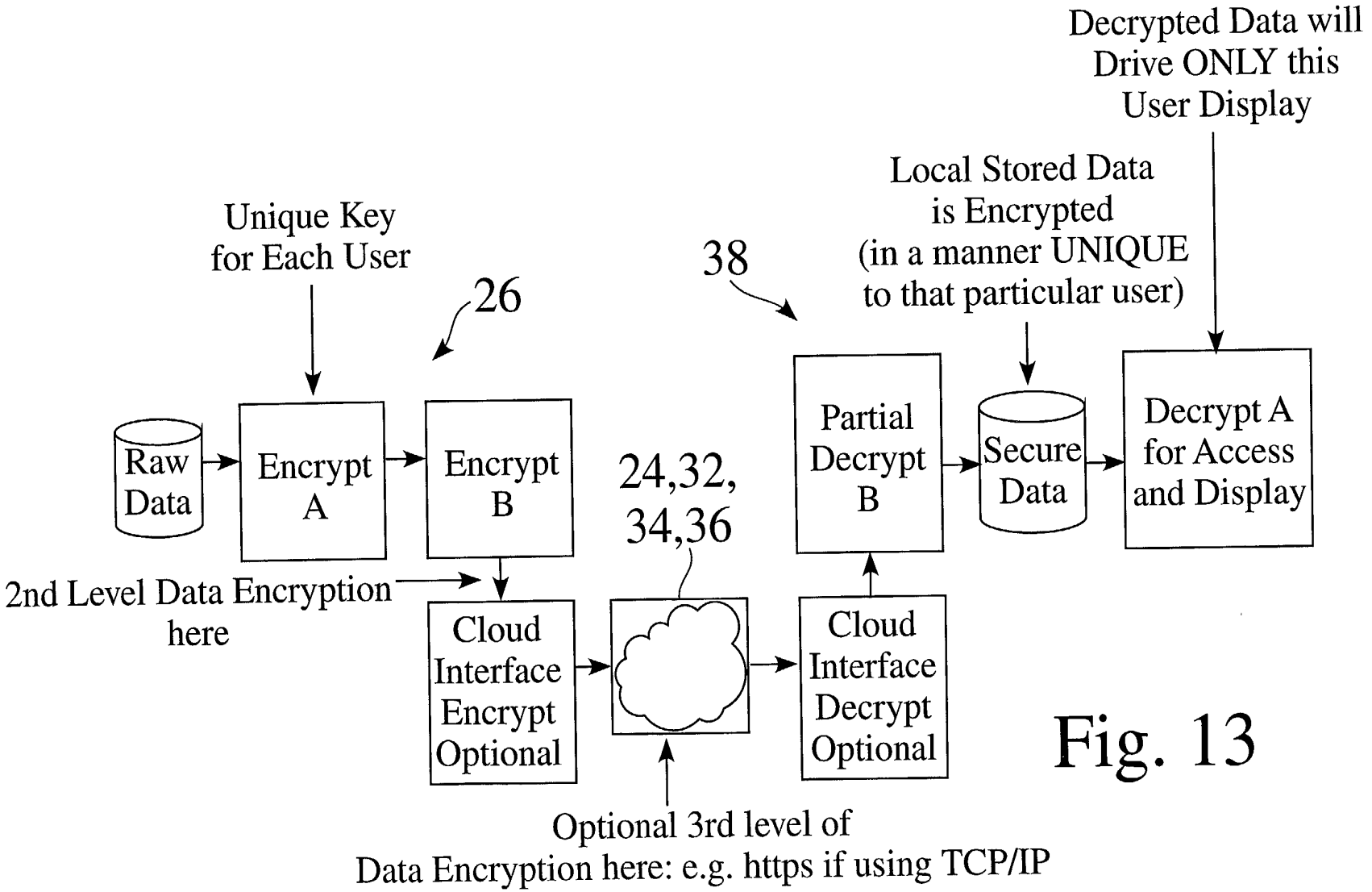

Decrypted Data will
Drive ONLY this
User Display
Local Stored Data
is Encrypted
(in a manner UNIQUE
to that particular user)
Unique Key
for Each User
38
26
Raw
Data
Encrypt
A
Encrypt
B
24,32,
34,36
Partial
Decrypt
B
Secure
Data
Decrypt A
for Access
and Display
2nd Level Data Encryption
here
Cloud
Interface
Encrypt
Optional
Cloud
Interface
Decrypt
Optional
Optional 3rd level of
Data Encryption here: e.g. https if using TCP/IP

Fig. 13

System Server Functions

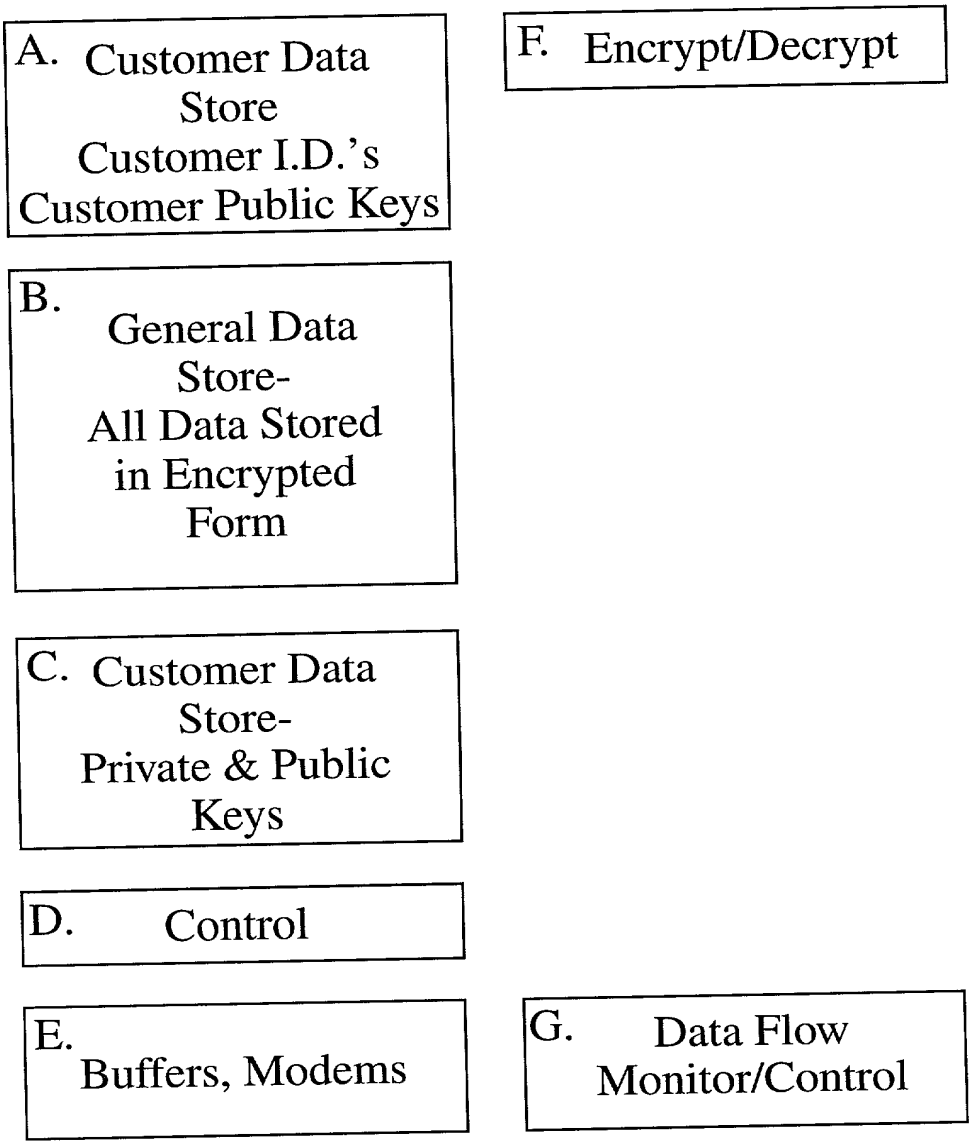


Fig. 14

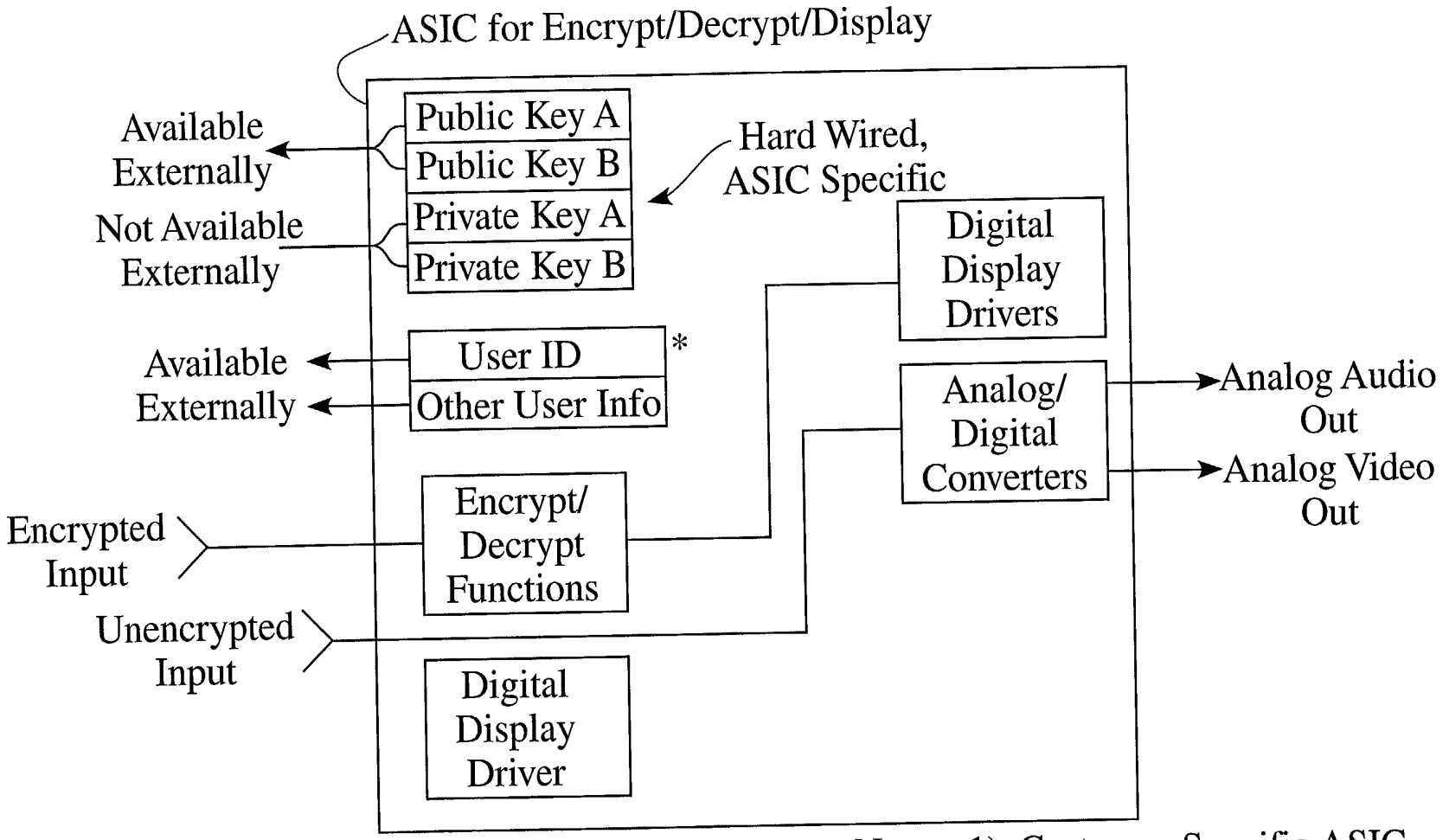
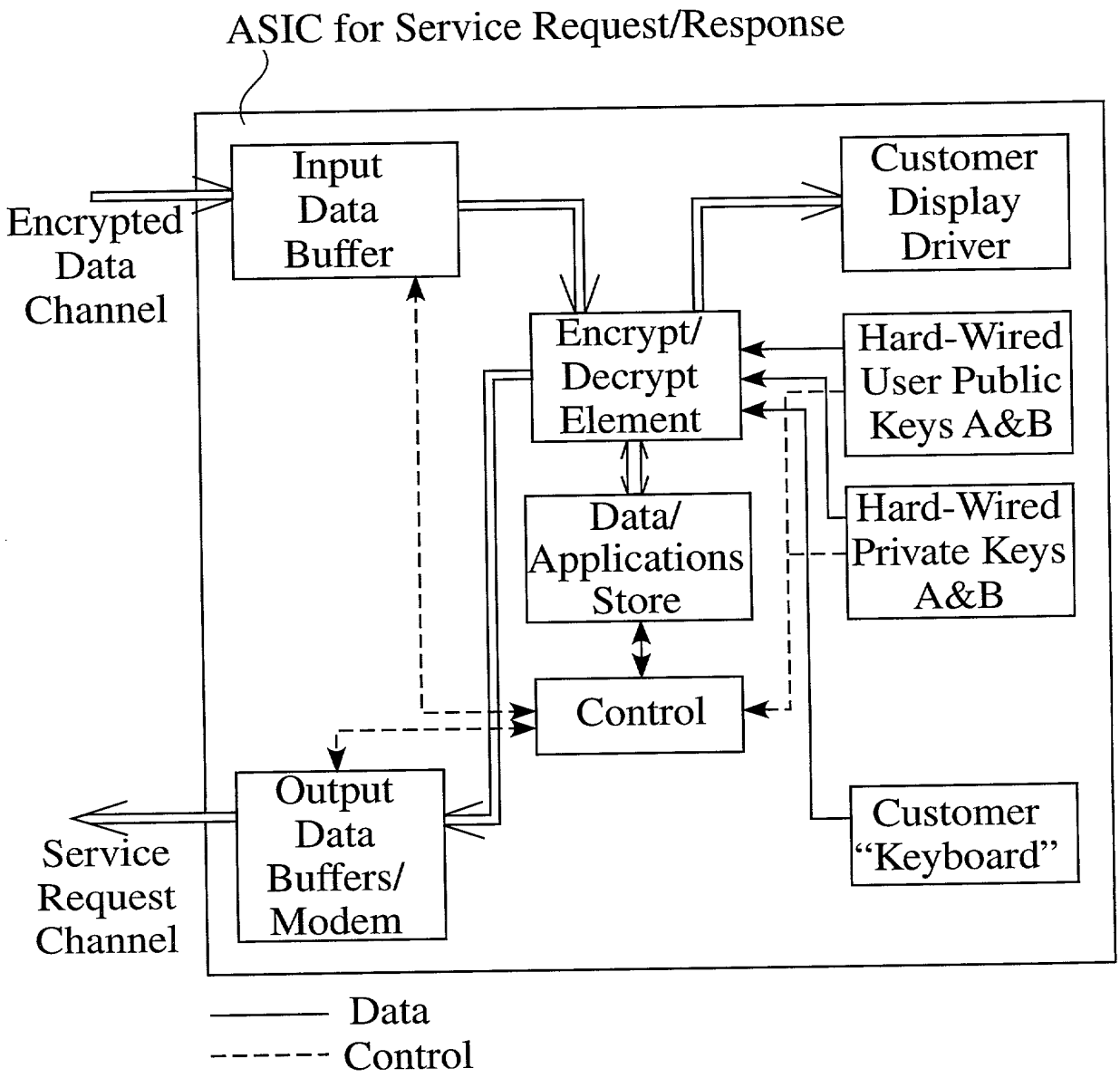

ASIC for Encrypt/Decrypt/Display
Public Key A
Public Key B
Private Key A
Private Key B
Available Externally
Not Available Externally
Hard Wired, ASIC Specific
Digital Display Drivers
User ID
Other User Info
*
Available Externally
Analog/ Digital Converters
Analog Audio Out
Analog Video Out
Encrypt/ Decrypt Functions
Encrypted Input
Unencrypted Input
Digital Display Driver
* May Be Stored Externally
Notes: 1) Customer-Specific ASIC, Analog & Digital Circuits
2) No Digital, Decrypted Data Available External to ASIC

Fig. 15



Notes: 1) Request for Data - Control sends Public Keys A&B to System Sources via Output Data Buffer; sends Data I.D. Number to identify stored data upon receipt.
2) Data Reception - Control identifies Data & applies Private Keys A or B for Storage or Display.

Fig. 16

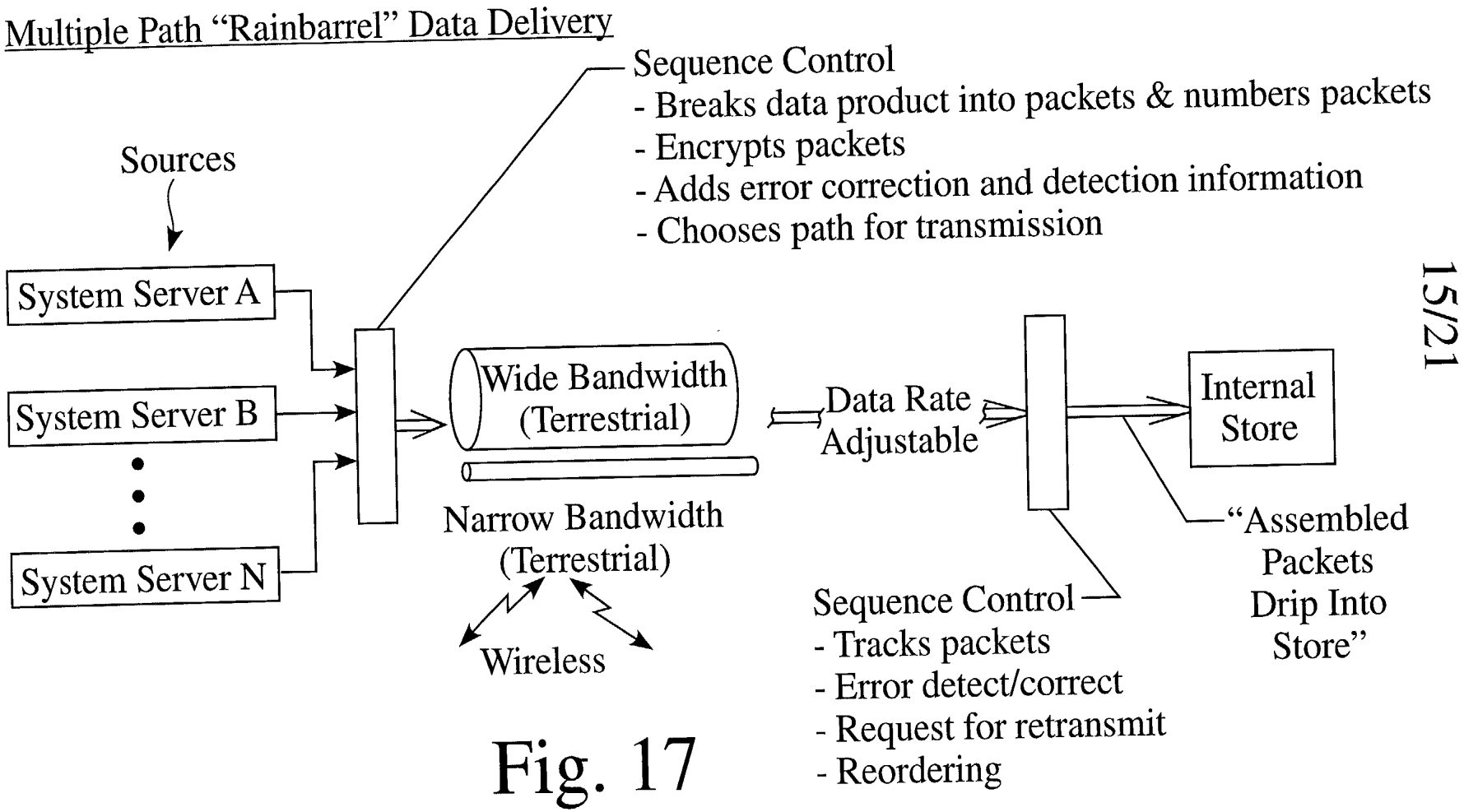

Multiple Path "Rainbarrel" Data Delivery
Sequence Control
- Breaks data product into packets & numbers packets
- Encrypts packets
- Adds error correction and detection information
- Chooses path for transmission
Sources
System Server A
System Server B
System Server N
Wide Bandwidth
(Terrestrial)
Narrow Bandwidth
(Terrestrial)
Wireless
Data Rate
Adjustable
Internal
Store
"Assembled
Packets
Drip Into
Store"
Sequence Control
- Tracks packets
- Error detect/correct
- Request for retransmit
- Reordering

Fig. 17

Request for Data and Response

1) Customer requests data menu from system server.

2) System server responds with menu, etc.

3) Customer requests "data".
   - Generic request: customer sends customer ID, public key A; encrypts by public key.
   - Requests for specific data: customer sends ID, public keys A and B; encrypts by public key

4) Network encrypts/decrypts (for example, with https); system server decrypts and searches data base for response.

5) System server extracts data, "packetizes" the data.
   - Server encrypts the data with public key A
   - Network encrypts/decrypts

6) Network operating system routes encrypted packages over available routes to customer.

7) Customer decrypts with private key A
   - Generic request: Display menu
   - Specific request: Data buffered, reassembled and stored in encrypted form.

Fig. 18

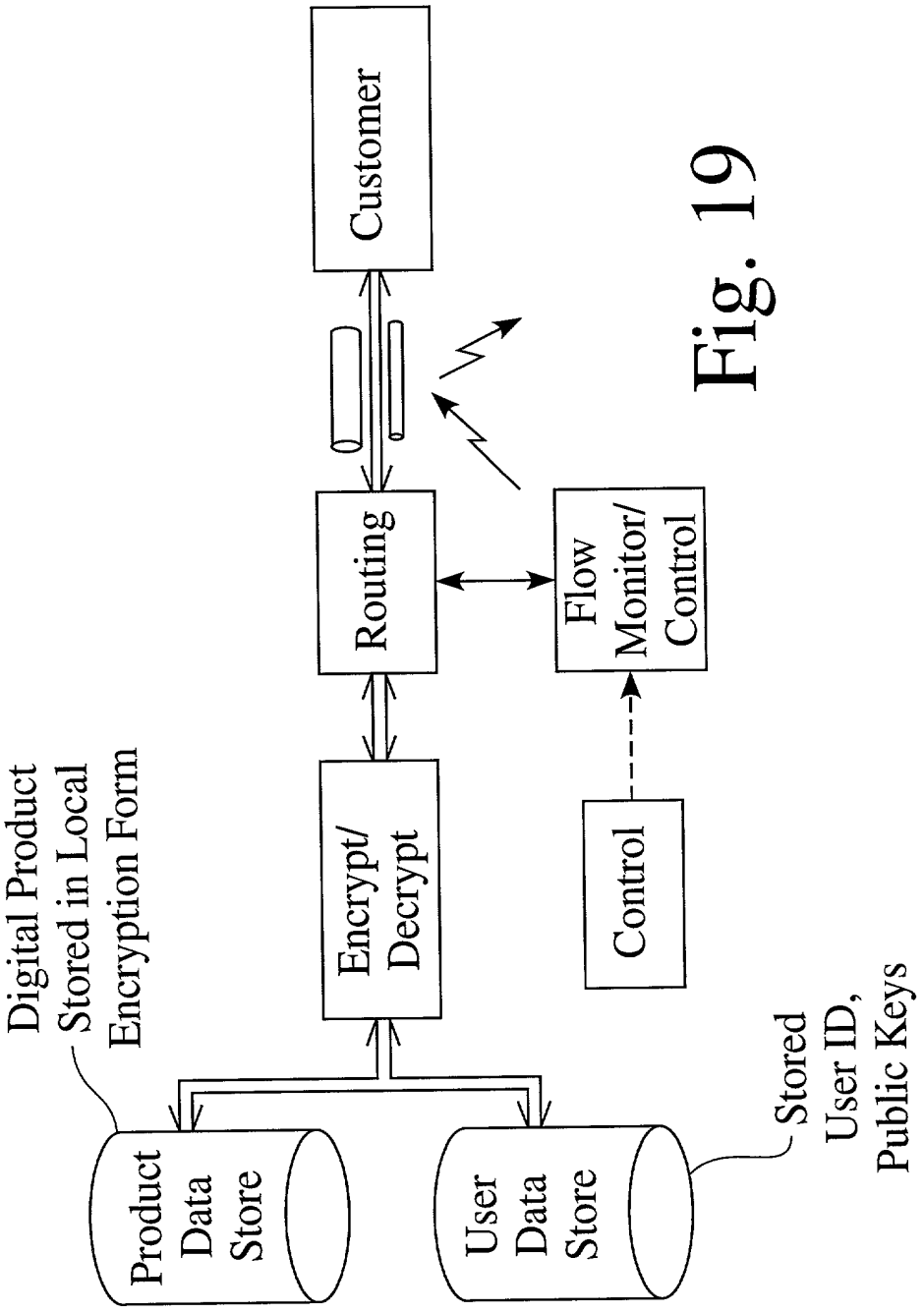
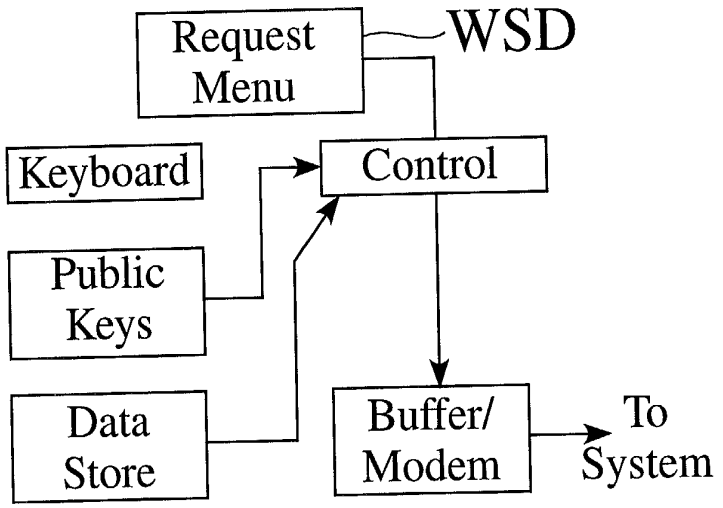

Customer
Routing
Flow Monitor/ Control
Encrypt/ Decrypt
Control
Digital Product Stored in Local Encryption Form
Product Data Store
User Data Store
Stored User ID, Public Keys

Fig. 19



1) At request for system menu, the following actions occur:
   - Control extracts user ID, public keys A&B from user hardware
   - Control extracts software application containing data request protocols from Data Store and directs request to Output Data Buffer/Modem.
   - Encrypted request is transmitted to a system server via available channel.

   - Additional encryption is available using https when using TCP/IP protocols over the channel.

2) At receipt of menu data, Control decrypts with private key B and stores in Data/Application Store.
3) When data transfer is complete, Control causes display to indicate "Menu Available."
4) Customer requests menu display from the keyboard (or mouse, etc.)
5) Control extracts encrypted data from Store and performs second decryption using private key A.
6) Data is displayed on screen, but digital unencrypted form of the data is unavailable outside of display ASIC.

Fig. 20

User Request for System Data

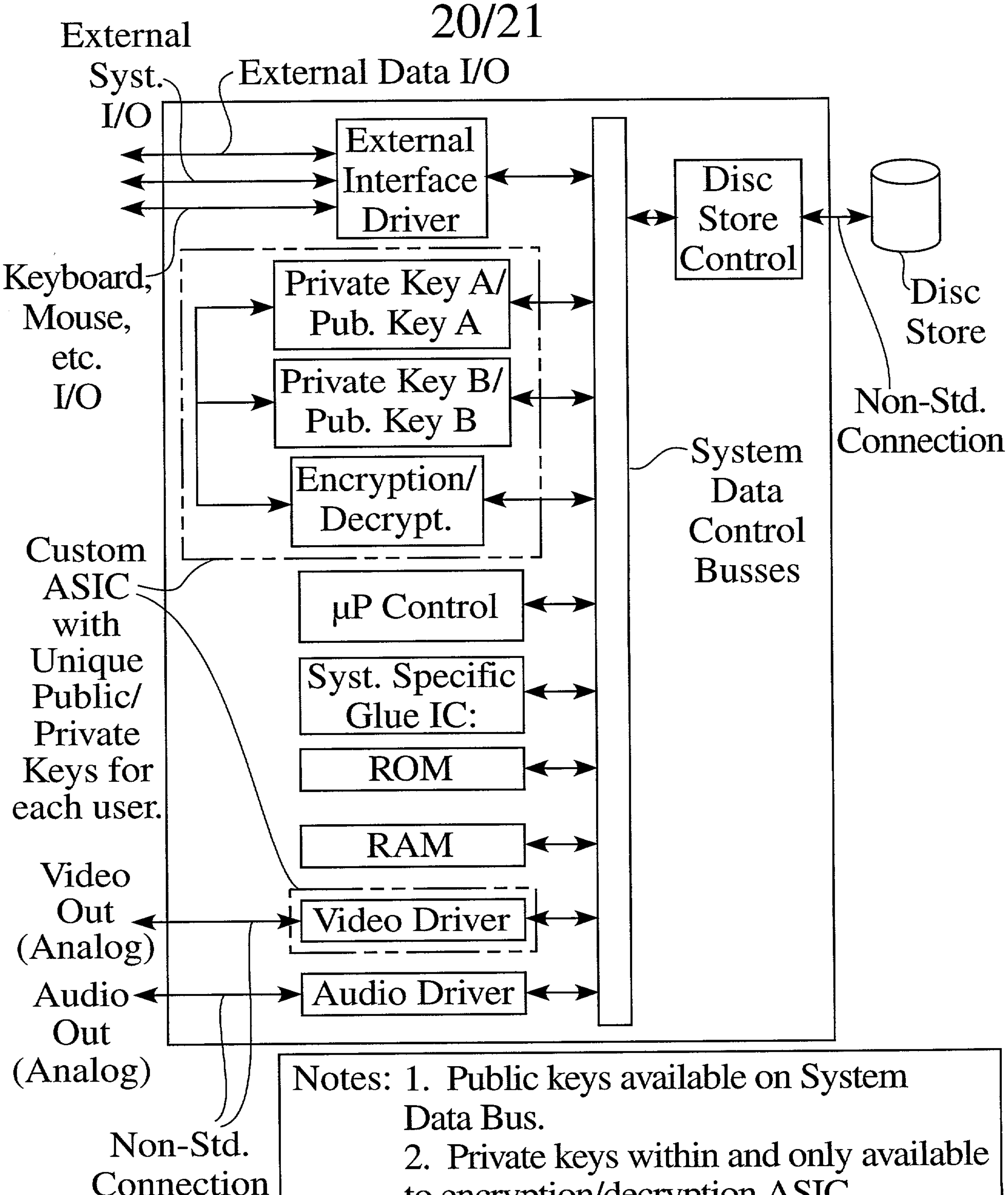
1) Customer requests system menu data by keyboard (or mouse, etc.)
2) Request is encrypted using public key A and stored in Data/Applications Store. Customer ID, public keys A and B are attached.

3) Request is also encrypted using System public key and sent to Data Flow Monitor/Control and Buffers/modems for transmission via available digital channel.

4) At receipt of data request by System, the following actions occur:
- Controller stores customer request in a General Data Store.
- Requested data is encrypted using customer public keys A & B and sent to Data Flow Monitor/Control for progressive transmission through buffers/modems.
- Selected least significant bits of data, controlled by customer public key, are altered with a **customer-specific** signature.

5) When customer receives data, Control decrypts data using private key B and stores blocks in Data/Applications Store. When all data blocks are received, Control notifies user via the display.
6) When customer requests to view the data, Control decrypts it using private key A and removes the digital signature. Control then sends the data to the display driver.
7) Note that all keys are hardware specific an not available to the operating system. They are usable only by the encrypt/decrypt/display ASIC. No "Hacker" access since digital data is never available outside the user's hardware.

Fig. 21



Notes: 1. Public keys available on System Data Bus.
2. Private keys within and only available to encryption/decryption ASIC.
3. Digital data never available outside of ASIC in unencrypted form.
4. All data stored on disc, or equivalent, is in encrypted form.
5. Analog video and audio data transmitted to off-board displays via non-standard connectors and cables.

Fig. 22

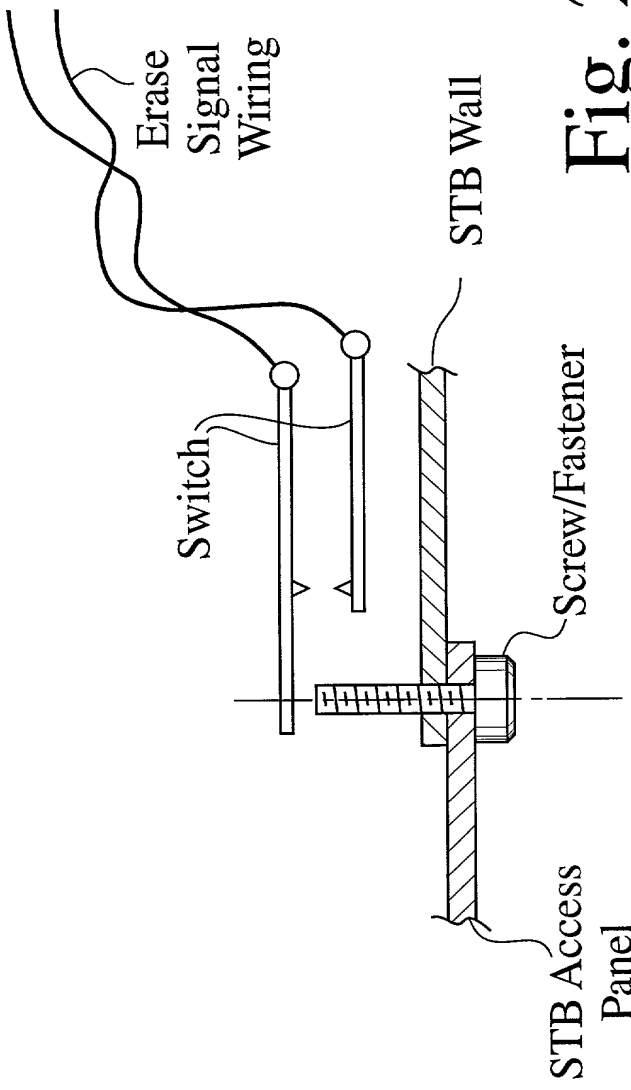

Erase
Signal
Wiring
STB Wall
Switch
Screw/Fastener
STB Access
Panel

Fig. 23